Fermilab Policy on Computing

Fermilab's Policy on Computing covers all Fermilab-owned computers and any device, regardless of ownership, when it is connected to our network (and/or showing a Fermilab address or representing Fermilab). You are responsible for the actions of any person whom you permit to use Fermilab computing or network resources through an account assigned to you. Note that discrete electronic devices that are not on the general network are not considered to be computers nor governed by this policy document. Devices used in Safety Instrumented Systems are covered by requirements listed in the Fermilab Work Smart Standards.

Fermilab's Computing Policy is a set of mandated user and system behaviors designed to:

- operate an effective and efficient computing and networking environment;
- maintain an open environment supporting global collaboration and innovation and free exchange of scientific information;
- guard the laboratory's reputation and protect its computing systems, data, and operations against attacks and unauthorized use;
- ensure compliance with all applicable mandates, directives and legal requirements for computing.

The Computing Division has been assigned the responsibility for the laboratory's computing and networking infrastructure. Complete details of the various policies can be found by following the appropriate links at http://security.fnal.gov/Policies which are maintained by the Computing Division.

Policies Governing Personal Conduct

Appropriate Use

All computer users are required to behave in a way that maintains the security of the laboratory computing environment. In particular, unauthorized attempts to gain computer access, to damage, alter, falsify, or delete data, to falsify either email or network address information, or to cause a denial of computing or network service are forbidden. Laboratory computers should only be used for laboratory business with exceptions made for limited incidental use consistent with this policy.

The following activities and uses are explicitly NOT permitted:

- Legally prohibited activities;
- Activities that reasonably offend other employees, users, or outsiders, or results in public embarrassment to the laboratory;
- Activities in support of an ongoing private business;
- Up- or down- loading or viewing of sexually explicit material.
- Computer usage that is not specifically approved and which consumes amounts of computer resources not commensurate with its benefit to the laboratory's mission or which interferes with the performance of an employee's (or other computer user's) assigned job responsibilities;
- Violation of license and other computer related contract provisions, particularly those that expose the laboratory to significant legal costs or damages.

Not explicitly prohibited but likely to get you into immediate trouble through embarrassment to the laboratory are all activities on newsgroups, auctions, game sites, etc. that are not clearly Fermilab business, all such Internet activities that are in competitive and/or contentious environments (e.g., auctions, political news groups, etc.) and using your computer to act as a public server of music or other media unrelated to our mission.

Questions of proper or improper use of computers are normally management rather than computer security issues and should be handled in the normal course of supervisory oversight.

More details about the lab's appropriate use policy can be found in the Cybersecurity Acceptable Use policy at https://cd-docdb.fnal.gov/cgi-bin/sso/ShowDocument?docid=7085

Incident Reporting

You are required to immediately report any suspected computer security incidents to 630-840-2345, or, if immediate response is not required, to cybersecurity@fnal.gov. The Fermilab Incident Response Team investigates incidents. The coordinator of the response team may assume full administrative control of affected systems until the incident is resolved, call on other experts for priority assistance and direct local system managers' response to the situation. Nothing should be done to the system before the response team has a chance to examine it. You may not disclose information regarding a computer security incident without authorization.

Information Handling

All users must comply with laboratory policies dealing with information categorization and protection, in particular with protecting personally identifiable information (PII). Details of these procedures are at https://cd-docdb.fnal.gov:440/cgi-bin/RetrieveFile?docid=2134&filename=PII%20Procedures-final.pdf&version=1

Data Integrity and Backup

Users ("data owners") are responsible for determining what data requires protection and how their data is to be recovered if the online copy is destroyed (either by accidental or malicious damage). They may choose not to back up data, but if so they must make sure they know how to recreate the lost data if needed. If backup is necessary then the users must coordinate a backup plan. This may either be an individual backup done by the users themselves or coordinated with the system managers into a regular system backup plan.

Security Training

All computer users must participate in periodic security training. System administrators will receive more advanced training.

Respecting Rights of Privacy

Fermilab respects the privacy rights of all employees and visitors, and will not look at any individual's private computer files without authorization from the lab director or designee except in a computer security emergency. Note that this policy does not apply to files in areas that formerly belonged to personnel who no longer maintain their previous association with the laboratory. In this case the file ownership is assigned to the person's former supervisor for appropriate disposition. In addition, it should be remembered that by connecting any computer to the lab network or using the Fermilab assigned names or IP addresses, the individual has waived their privacy rights with respect to the Department of Energy (as stated in the logon banner present on all lab devices), and even personal or university owned devices are subject to confiscation in a DOE Inspector General investigation.

Policies Governing Computing Systems

System and node registration

All devices attached to the lab network must be registered and have a registered system administrator with an up-to-date email address. The system administrator is the individual responsible for applying security patches to the device and choosing system configuration.

Visitors will be given an opportunity to temporarily register their devices when they first request a DHCP address by connecting to the lab network. They will be granted access unless a critical vulnerability is detected on their computer (see http://security.fnal.gov). In that case they will need to physically take their device to the help desk in Wilson Hall (where an offsite network connection is available to allow them to patch their device) or mitigate the vulnerability in some other manner.

Virus Protection, Patching and Configuration Management policy

The policies in this section apply (unless otherwise noted) to all laboratory networks other than the guest network.

All lab-owned or network attached systems must provide appropriate endpoint protection (anti-malware, local packet filtering, removal of unnecessary network services) as specified in http://security.fnal.gov/Policies/EndpointProtectionPolicy.htm.

All lab Windows computers, OSX computers or computers offering Windows file shares must have enabled virus scanning software and must have a plan for applying security patches and updating virus signatures. Devices in the Fermi Windows domain satisfy this requirement, as do those subscribing to one of the lab SMS servers; for other devices users must supply documentation of how this requirement is met. The full aniti-virus policy is given at https://cd-docdb.fnal.gov:440/cgi-bin/ShowDocument?docid=1136

Computing systems should be running recent and supported versions of operating systems, regardless of network connectivity, as specified in the lab configuration management policy and listed baseline configurations that can be viewed at: https://fermipoint.fnal.gov/org/cs/pages/computer-security-documents---general-computing-environment.aspx

It is recognized that in some circumstances it may be necessary to continue to run an obsolete operating system (for example, to avoid breaking software applications). In those cases the user of such systems must document the reasons why the system cannot be brought up to date and must document how the system is protected to provide the same level of security as provided in baseline configurations. A service desk ticket requesting a baseline variance and providing the required information should be opened in such cases. In addition, certain services (such as web servers) cannot be offered on such obsolete systems.

The Fermilab Information System Security Officer (ISSO) may declare, when deemed necessary for protection of Fermilab computers and users, that certain configurations are considered to be a Critical Vulnerability. This designation and the corresponding corrective action will be publicized widely in email and at the link below. You are required to take immediate action to remove Critical Vulnerabilities from systems under your control. Failure to comply will result in the system being blocked from network access. The current list of critical vulnerabilities can be seen at:
http://security.fnal.gov

It is expected that computer users will practice "least privilege required", in particular only using administrative or root accounts for limited periods of time when conducting activities that require such privileges.

Restricted Central Services

Services that would create a significant security risk or would interfere with the operation of site computing or networking infrastructure can only be operated by systems authorized by the Fermi Security Team.

For example, the following network services may only be implemented by the Core Computing Division (see DocDB item 4265 for more examples):

- Routing and bridging, unless exempted.
- Tunneling, except tunnels with a single source or destination for purposes of mobility or security.
- All forms of off-site network connection except modems.
- DHCP servers.
- Wireless access points
- Assignment of IP host names and addresses. (Use of automatic configuration mechanisms provided by the lab networking, such as DHCP, are not restricted.)
- DNS zone mastering and all externally-reachable DNS service.
- NTP time service at stratum 1. (Stratum 2 server operation is discouraged.)
- NNTP.

Specific waivers from these restrictions must be requested through the Service Desk ticketing system and may be granted only by the network manager or the Fermilab Information System Security Manager (ISSM). Waivers granted to non-Fermilab employees require the concurrence of the Fermilab CIO.

The following services are also examples of restricted services. (Exemption requests for professionally managed workgroup-local implementation will be considered by the ISSM.):

- Externally-reachable or onsite email servers, including SMTP, POP and IMAP
- Kerberos key servers
- Active directory servers
- VOMS, GUMS and SAZ servers
- Federation Authentication Servers

Furthermore, externally visible web services, including project and personal web pages, should only be offered on one of the central lab web servers. If necessary, a user can request permission to run a private

web server by opening a “Web Hosting Request” through the Fermilab Service Desk at:
https://fermi.service-now.com/wp/

This will require up-to-date security scans demonstrating that the proposed web server runs on a secure device. Web traffic to other-than-registered servers will be blocked at the site border.

Externally visible Globus gateways must also be registered and approved before being put into operation, and will normally be restricted to the Open Science Enclave.

Care must be taken with web content on both private and central servers. See http://directorate-docdb.fnal.gov/cgi-bin/RetrieveFile?docid=31. Owners of web pages are responsible for any posted content, and are required to institute procedures (e.g. authentication) that will discourage posting of dangerous or embarrassing content. Use common sense in displaying links on pages with Fermilab addresses. Web crawlers (Yahoo, etc.) index all pages they can see. Even accidentally inappropriate wording may be indexed. You can direct web crawlers to ignore pages that you do not need to be found t through search engines. See https://fermi.service-now.com/kb_view_customer.do?sysparm_article=KB0010588. Semi-official pages and pages intended for the public are required by the DOE to carry a notice. Include a link on each such page to http://www.fnal.gov/pub/disclaim.html

A complete current list of restricted services can be found at http://security.fnal.gov/Policies.

Bypassing Central Services

The Laboratory invests significant resources into maintaining services that are managed centrally which are critical to the main operations of networking and communications and general application stability. When performing Fermilab business, a user must utilize the central services that are offered. Attempts to utilize 3rd party services or applications that compete with Central Services for business purposes may result in the service or application being unavailable from proactive controls. In some cases access to external services of these types are blocked at our site border; in other instances attempted access to such an external service could result in the system making this access being blocked from the lab network.

A current list of such external services and the actions resulting from attempted access can be found at http://security.fnal.gov/Policies.

Access Control

All applications, other than those intended for the general public, must support appropriate levels of authentication and authorization. In particular, any systems allowing arbitrary program execution or data transfer require authentication consistent with computing authentication policy at https://cd-docdb.fnal.gov:440/cgi-bin/ShowDocument?docid=3172, currently either a Kerberos principal (account) for use of general lab computing resources, or a PKI certificate for use of grid computing resources. You will need to understand how to authenticate yourself through proper use of your credentials before being able to use lab computers. The Authentication Policy document also gives the current lab regulations on use of passwords.

You must not allow anyone else to know or use your Kerberos password. Do not use your Kerberos password for other than Fermilab Kerberos. Do not transmit Kerberos passwords across the network. In the rare circumstances where transmitting a Kerberos password is necessary, it must be strongly encrypted. Never store Kerberos passwords (or the corresponding character strings) on a computer, encrypted or not.

Passwords are to meet or exceed the password complexity and lifetime requirements defined in DocDB 3108, with the exception of the Kerberos password which has a longer lifetime. Do not store Fermilab passwords within the browser password store. Do not re-use Fermilab passwords for other services. If you utilize a password store in your browser or a password wallet, be sure to encrypt it with a strong passphrase.

Any remote login or general file transfer services in the General Computing Environment that are visible from outside the Fermilab network must be configured so as to require Kerberos authentication (or an exemption must be requested). See https://cd-docdb.fnal.gov:440/cgi-bin/ShowDocument?docid=3172 for more details. Configuration rules for Kerberos-protected systems must not be circumvented. Similar services in the Open Science Environment must be configured to require appropriate grid certificates.

Encryption Standards

Any use of Encryption methods must utilize current methods with a strength applicable to the level of sensitivity of information being protected.

Any electronically transmitted or portable (e.g. thumb drives, CD's) authentication credentials, Business Sensitive information or PII data must utilize encryption methods.

Business Sensitive or PII data at rest in the originating system may utilize data at rest encryption methods, if available. Downloaded Business Sensitive or PII data at rest on a non-originating system shall utilize data at rest encryption methods.

Communications between general support systems may utilize encryption mechanisms, with a strength applicable to the data being transmitted.

Policy Enforcement

Individuals who violate this policy will be denied access to laboratory computing and network facilities and may be subject to further disciplinary action depending on the severity of the offense.
Computing systems with critical vulnerabilities, that exhibit unusual network behavior typical of hacking activity, or are otherwise in violation of this policy will be blocked from network access until the condition is mitigated.

Software Intellectual Property (Licenses)

Employees and users of Fermilab computing are reminded that it is Fermilab policy to respect the intellectual property rights of others. This applies when computers are involved just as it does when computers are not involved. Fermilab expects license provisions to be followed.

Disclaimer

In using systems owned by Fermilab or attached to the Fermilab network, users waive their rights of privacy with respect to information on those systems, and accept the possibility of loss, damage or disclosure of any data, including their own, on those systems.

Use of Computers in Systems that Protect People, Property, or the Environment

It is Fermilab policy to avoid reliance on a computer as an essential element of any system that is necessary to protect people from serious harm, to protect the environment from significant impact, or to protect property the loss of which would have a serious impact on our mission. The use of computers for monitoring, data logging, and reporting is encouraged, however computers used for these purposes must not be essential for protection. Contact the Fermilab Computer Security Executive for any variance.

Further details on the various policies referred to here can be seen by following the links at:
http://security.fnal.gov/Policies

Oct 17, 2019